KEYLOGGER WITH ENCRYPTED DATA EXFILTRATION

INTRODUCTION

This project focuses on developing a Python-based keylogger designed to capture and record keystrokes on a system for cybersecurity research and awareness purposes. The goal of the project is to demonstrate how keylogging attacks operate, how sensitive data can be exfiltrated, and how encryption can secure logged data from unauthorized access

ABSTRACT

The Keylogger with Encrypted Data Exfiltration project demonstrates the mechanics and security implications of keylogging software within an ethical research context. Implemented in Python, the tool captures system keystrokes in real time using pynput and stores them in a protected log. Captured data is encrypted with Fernet (from the cryptography library) to ensure confidentiality and then encoded with Base64 for safe storage and transport. The project is designed as a learning and defense-oriented exercise: it clarifies how keyloggers operate, illustrates secure handling of sensitive logs, and highlights detection and mitigation strategies to strengthen endpoint security.

TOOLS USED

- Python 3.14.0 is the version of python used for developing this project.
- Pynput is provided by python library used to capture the keyboard inputs
- Fernet is symmetric encryption scheme provided by the cryptography library. It gives you authenticated symmetric encryption (confidentiality + integrity) in a few lines
- Base64 encodes encrypted bytes for secure file storage and transport

STEPS INVOLVED IN BUILDING THE PROJECT

1. **Environment setup and dependency installation**
   Set up the python environment and installed the required libraries like pynput, cryptography, base64 for the project
2. **Secret key generation and management using Fernet**
   Created a secret key using Fernet module from cryptography library for secure encryption.

The system generates a strong symmetric key using a modern authenticated-encryption scheme and persists it to a single key file that the application can reuse for subsequent runs

3. **Keystroke capture with a keyboard listener**
   Captured key strokes using the pynput. keyboard listener
4. **Encryption of captured data and Base64 encoding for storage**
   Encrypted each keystroke along with timestamp and stored it in an encoded format using Base64
5. **Safe shutdown mechanism (ESC kill switch)**
   To ensure the capture process can be stopped cleanly and predictably, a designated kill switch was implemented: pressing the ESC key stops the listener and triggers a graceful shutdown routine.
6. **Simulated exfiltration of data by printing preview of encrypted logs to console**
   To demonstrate how encrypted logs would be prepared for transfer without performing any real network exfiltration, the project includes a simulation step that prints a truncated preview of encrypted entries to the console.

Maintained Ethical usage as this tool is for defensive research and education only and must not be used on systems without explicit written authorization.

CONCLUSION

The Keylogger with Encrypted Data Exfiltration project successfully demonstrates the complete workflow of keystroke logging, secure data handling, and controlled data preview within an ethical cybersecurity framework. By developing this project in Python and integrating libraries such as pynput, cryptography (Fernet), and base64, the implementation effectively captures, encrypts, and encodes sensitive input data to simulate how attackers might collect and protect stolen information.

Note: Legal & Ethical Notice: *This project is developed solely for educational and defensive cybersecurity research. Do not run this software on machines you do not own, or without explicit written consent. Unauthorized capture of keystrokes is illegal and unethical.*